Ten-Stage Security Management Strategy Model for the Impacts of 'Security Threats on E –Business'

Narendra Kumar Tyagi
Research Scholar (CS)
Shri J J T University
Jhunjhunu, Rajasthan

Prof(Dr.)S.Srinivasan
PDM College of Engg.
Bahadurgarh, Delhi-NCR
Haryana

ABSTRACT
This paper is an attempt to give a high-level overview of security in the e-business world. e-Business includes informational websites that are being fielded on an almost daily basis by companies. This paper attempted to view security concerns as a problem to be solved with technology and main consideration is to which firewall or encryptography should use rather than formulating a security strategy. Technology is next to useless unless applied within a strategy, just as tanks are wasted without an overall battle plan. Some of the security threats areas, such as services advertising, require the implementation of only few, security controls, while others, like customer recruitment/registration, require more comprehensive controls, to ensure compliance with money and customer's requirements. This paper throws light into the kinds of various concerns a person should be worrying and providing a look at some of the security technologies available.

Keywords: e-business, Internet, Security, phishing, measurement, survey method, basic advanced technologies

1. INTRODUCTION
1.1What is e-Business:
E-business or Electronic business may be defined broadly of any business process that runs on the Internet. In more general way, it can be said that any business using computer is e-Business. But today it is mostly done using web, Intranets, Internet, Extranets or any combination of these so e-business refers exclusively to Internet business. [1] e-business includes informational websites that are being fielded on an almost daily basis by companies. It is not limited to just buying and selling but also servicing customers and collaborating with business partners [2]. A security plan is an absolute must for companies that are serious about protecting their assets while doing e-business.

To e-business security plans are unique and must be developed through a series of steps. While the plans are unique the steps taken by companies can be very similar.

1.2History
IBM, in October 1997, launched a thematic campaign built around the term e-business. Today, major corporations are rethinking their businesses in terms of the Internet and its new culture and capabilities. Companies are using the Web to buy parts and supplies from other companies, to collaborate on sales promotions, and to do joint research. Exploiting the convenience, availability, and world-wide reach of the Internet, many companies, such as Amazon.com- the book sellers and CISCO [3] have already discovered how to use the Internet successfully. As organizations start to exploit the benefits of the web technologies, they face inherent risks involved in connecting their organization's networks to the Internet. The process of exposing valuable data to a wider world significantly increases the risk of malicious attack. Jajodia et al. [4] describes the "Topological Vulnerability Analysis" (TVA) implementing an integrated, topological approach to network vulnerability analysis. On transformation, an organization's dependence on security, availability, and manageability increases. Businesses are exposing themselves increasingly with the wide use of the Internet to attract and service customers, coordinate and conduct transactions with suppliers. They mine for information about their customers and competition. A single employee, customer, or malicious individual has the power to touch data within the organization. This connectivity creates countless entry points and security threats and risks. Thus, security plays the role of protector and of e-business enabler as well as.

2. REVIEW OF LITERATURE
Research in any field implies a step ahead in exploration of the unknown. A step towards unknown can only be taken after the review of literature and researches done in that area. Any research without such a review is likely to be a building without foundation.

The review of past investigation serves as a guide to the researchers as it avoids duplications in the field. The knowledge of what has already been done in the area of investigation regarding the methods used for data. Collections and results of their analysis keep a researcher systematic in his own endeavor. Thus, the review of related literature is an indispensable step in research.

2.1. Anil Chopra and Anindya Roy
In (Anil, 2005) [5] has depicted that scam esters are finding new and more powerful techniques to gain access to your bank account information. The most common techniques are phishing and pharming that redirect you to fake website.

2.2. Avenue de Tervueren
In (Avenue,2004) [6] has described a set of guidelines for Secure Electronic Banking which are recommended to be

adopted by European Banks. This report identified five different e-banking services which are classified as five risk profiles. Some of the risk areas, such as services advertising, require the implementation of none, or only few, security controls, whereas others, like customer recruitment and registration, require more comprehensive controls, to ensure compliance with money laundering and "Know your Customer" requirements. Accent Vendor in (Vendor,2007) examined the top 10 security threats in 2007 facing by internet business that are phishing, kernel vulnerabilities, web based worms, targeted file attachments attacks, window file format attacks etc

2.3. CISCO

White Paper [4] concluded that small and medium sized businesses use the Internet and networked application to reach new customers and serve their existing ones more effectively. It depicted that the security is the biggest challenge facing small and medium sized businesses. According to it top 5 security issues are worms and viruses, information theft, business availability, the unknown and security of legislation [2]. Several Security standards and frameworks are available that are internationally developed, and are characterized as large, complex, all encompassing documents.

This paper shows that small and medium-sized businesses use the Internet and networked applications to reach the new customers and serve their existing customers more effectively. But the new security threats and legislation have put increased pressure on business networks to be reliable and secure. It observed some comprehensive, affordable, integrated security solutions tailored for small and medium-sized businesses that help ensure business continuity, maintain customer privacy, and reduce operating costs. The study of CISCO reveals that the companies can confidently spend more time growing their business, and less time focusing on network security issues.

The Cisco Self-Defending Network is the Cisco long-term strategy to secure business processes by identifying, preventing, and adapting to both internal and external threats. The Cisco Self-Defending Network protects businesses today and adapts to future needs. With Cisco, businesses can protect not only their networks, but also their network investments. The results are improved business processes and substantial savings. This is a simplified yet comprehensive, cost-effective security solution for small and medium-sized businesses that creates reliable and self-defending networks.

2.4. C.T. Upfold and D.A. Sewry

In [7] found that Information systems and technology, originally considered to provide businesses, both small and large, with decision support advantages, are now operational imperatives. The widespread adoption of Internet technologies is enabling SME's to connect to one another and to large business, both locally and globally. While on-line banking, Internet access and email are now commonplace in SME's, they are increasingly adopting Elecronic Data Interchange (EDI), and Electronic Businesses (E-Business). SME's are not currently addressing information security adequately. Although SME leadership are aware of the need for information security, in many cases, this awareness is superficial. Virus protection and data backups (untested) are common amongst many SME.s, however, Security interventions in SME's are generally unplanned and ad-hoc. SME's must formalize information Security by adopting a Security standard. Several Security standards and frameworks are available that are internationally developed, and are characterized as large, complex, all encompassing documents.

3. OBJECTIVE OF SECURITY THREATS ON E-BUSINESS

The main objective of this study is to collect and analyses the views of Internet users that perform business transactions on Internet with regards to the impact of security threats on e-business. An e-business can not expect perfect security to be obtained for its network. The security objectives are the goals that are to be achieved in e-Business, on other side security services are means to achieve these goals. Traditionally, when dealing with data security, three security objectives are addressed: confidentiality, integrity, and availability. The individual with whom you are communicating may be masquerading as someone else. The result could be diversion of funds, loss of confidential information, and repudiation of contracts and so on. Present study concentrated upon gauging the Impact of Threats to Internet users. Specific objectives are-

- To explore the usage pattern of Internet services.
- To categorize various threats on basis of their potential to jeopardize internet users.
- To find out the percentage of users adopting security measures.
- By using security provisions, internet users are able to face the security challenges.

4. RESEARCH METHODOLOGY

It is necessary to get at facts firsthand, at their source and activity to go about doing certain things to stimulate the production of desired information. In this study of research, Survey method has been followed. To achieve the above mentioned goal and to collect the relevant data/information about the research topic, a questionnaire was developed using criterion test.

5. SURVEY: OBSERVATIONS

A 2001 Computer Security Institute (CSI)/ Federal Bureau of Investigation (FBI) survey of U.S. corporations, federal agencies, universities, and financial institutions on security problems revealed that:

– 94% were hit by a virus
– 70% had their Internet connection a frequent point of attack.
– 85% detected security breaches in the last 1 year.
– 40% had unauthorized access by an outsider.
– 64% had financial losses due to security breaches.

These 2001 figures are up in every category from 2000 which have risen consistently in the last five years. This only reflects the known attacks. The vast majority of computer crimes go undetected.

e-Business Security Threats issues touch every corporation. Businesses had safes, locks, and keys before there were

computers. The locks and keys terms are used to describe e-Business security trends. It might be possible to have at least limit access to software and systems or physically secure a company's data.

In 1991 the restriction of commercial use of the Internet was lifted and that marked the beginning of the era of E-Business. The 1999 CSI/FBI survey indicates that 55% of respondents had unauthorized access by employees, 40% (2001) of respondents had unauthorized access by an outsider and 25% (1999) had theft of proprietary information. The incipient growth was turbo charged with the development of the World Wide Web and GUI-based browsers shortly after [8]. This gives birth to simple and scalable network design offering a best-effort service, where the network does not guarantee anything, not even delivery of the data.

6. PROPOSED SOLUTION FOR SECURITY THREATS

Everywhere in e-Business, security is viewed as key business driver. Planner is a special purpose search algorithm for finding out a solution from initial state to goal state within a large state space. Using planner [9] from artificial intelligence domain has many advantages that adds interoperability [10] and an easy to use uniform user interface.

It is clear that there is no defense better than a comprehensive security strategy that embraces user education, crisis-response teams, and technologically sound security measures including those that relate specifically to the threats posed by viruses and worms. Protecting computers against viruses and spyware[11] should be done before start using any program on it. e-Business security is effective only if it is maintained as part of an overall corporate risk management policy.

Conduct audits, reassess and refine the plan and process at regular intervals. For that the eight-stage security management strategy [12] is enhanced to ten-stage security management strategy model, additionally with basic advanced technologies as given below:

6.1 Identify Security plan

Identify the security plan and process owner before starting.

6.2 Evaluate Risk

Evaluate- what is at risk & its value?

6.3 Evaluate Expenses

Evaluate- what the company should spend on risk protection.

6.4 Find Attacker

Find- who wants to damage through access?

6.5 Decide Security Vulnerabilities

Decide- the company security vulnerabilities (through self-exam and outside audit).

6.6 Evaluate Technologies

Evaluate- technologies & procedures (to close the drawbacks & tighten prevention).

6.7 Consider Attack Detection

Consider- how attacks will be detected.

6.8 Decide Action on Attack

Decide- what actions will be triggered on attacks

6.9 Educate Employees

Educate- employees continuously on the plan.

6.10 Appraise Insurance

Appraise- the use of insurance.

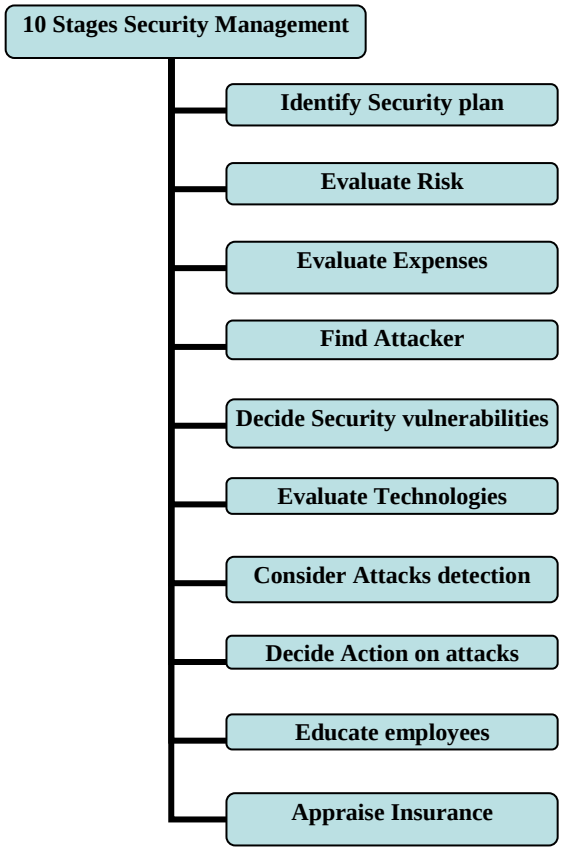

Fig1: Ten-stage Security Management Strategy Model

6.11 Basic Advanced Technologies

The Agent-Based Attack Simulator (ABAS) [13] is a multi-agent system[14] technology which uses two classes of agents: the "Network Agent" that simulates an attacked computer network and the "Hacker Agent" which a hacker performing attacks against the computer network.

Following are the basic advanced technologies used for Security Threats on e-Business-

- Encryption
- SSL and HTTP
- Application Security
- Authorization and Authentication
- Digital Signatures and Digital Certificates
- Securing the Database

- The Full Monty: PKI
- Firewalls and DMZs [15]

7. FUTURE SCOPE

The advanced technologies are useful for the various categories of persons who use computers and the Internet for attacking and stealing information creating the serious impacts of security threats. Knowing who is attacking can help determine the better way to keep them away. Police and government agencies with e-business companies are going to be benefited with these advanced technologies applications in controlling the impacts of security threats from inside as well as from outside. It is also true on the humanity side that security policies and procedures coupled with a good deal of education are the best defense against social engineering and human nature.

Security in E-business with controls has to be balanced with performance. The basic principle in designing with safety decisions becomes more important in case of security, safety and dependability otherwise it may lead dangerous situations of maintenance of e-Business [16]. Zero defect approach for nullifying the impacts of security threats in e-Business using cryptography and e-business policies[17] is the critical application against a reliability growth to eliminate faults in early stages for maximization of process and product methods. There is an urgent requirement for the defensive program against computer virus attack to guide design of dependable software, abstraction hiding, and fault tolerance with safety, dependability and integrity.

8. CONCLUSION

Security threats in e-Business are just a journey, not a destiny. It is a process of dealing in a war where careful assessment/tendencies of our opponent with a frank look at our own terrain and vulnerabilities are required before taking any defenses. Here clear rules, policies with procedures are to be thoughtfully derived and delivered to the companies. It is the skillful spreading of selected technologies which are configured correctly, and updated continuously. Security is the counter to the necessity of opening the enterprise to the great wide world of the Internet which is associated, anyway, to e-Business. The technological approach is not sufficient to produce trust or minimize risk so as to cause companies and their clients to conduct e-business with confidence. A risk management approach with safety, dependability and measurement is presented. Hence the chances are at most requirement that the market engaged with e-business will welcome this approach.

9. REFERENCES

[1] Bajaj, k kamlesh, And Nag, debjani "E-commerce The cutting edge of Business", Tata mcgraw hill, pp 197-200 (2002).

[2] Bichler Martin "Future of E-Markets Multi Dimensional Market Mechanism" Cambridge University Press, U.K., pp 17-20 (2001).

[3] CISCO "Top five security issues for small and madiem sized business", Cisco white paper http://www.cisco.com/en/US/ns643/networking_solutions_white_paper0900aecd804606fc.shtml (2005)

[4] S. Jajodia, S. Noel, B. O'Berry. "Topological analysis of network attack vulnerability", in *Managing Cyber Threats: Issues, Approaches and Challanges*, V. Kumar, J. Srivastava, and A. Lazarevic (eds.), Springer, Germany, (2003).

[5] Chopra, Anil and Roy Anindya "New threats to online banking". Pcquest, pp62-67 [July, 2005]

[6] Tervueren Avenue de, "Security guidelines for E- banking" (August, 2004).

[7] Upfold C.T. and Sewry D.A.(2005), "An Investigation of Information Security In Small And Medium Enterprises(SME's)In Eastern Cape" http://icsa.cs.up.ac.za/issa/2005/Proceedings/Research/082 Article.pdf

[8] "Life on the Internet", http://www.pbs.org/internet/timeline (2001).

[9] S. J. Russell, P. Norvig, "Artificial Intelligence: A Modern Approach", Prentice Hall, New Jersey, (1995).

[10] Narendra Kumar Tyagi, research paper "e-Bus : web services" in International Conference "icsci-09" held in Hyderabad (7-10 Jan, 2009)

[11] Narendra Kumar Tyagi, "Data Security from Malicious Attack: Computer Virus", BVIM Indiacom2010 (Track 2: Web Technologies, Computer Networks & Information Security (G -III)) National conference Proceedings at BVICAM, Paschim vihar, New Delhi (26-27th Feb 2010)

[12] For a similar approach see US GAO (1999).

[13] Narendra Kumar Tyagi, "Encountering with security Threats in e-Business using Agent Based Attack Simulator" International Conference at DIAS Rohini, Delhi on 3rd January 2011.

[14] Narendra Kumar Tyagi, research paper, "Database Security from Malicious Attack: Multi Agent System Approach" in AICTE sponsored National Seminar on Artificial Intelligence NSAI-09 proceeding (17 july 2009).

[15] Search Security.com, Firewall, available at: www.progress.com/webspeed/whitepapers/securing_firewall.htm

[16] Narendra Kumar Tyagi, "Security Threats in e-Business with Safety and Dependability", "Global Journal of Enterprise System (GJEIS)" July2010-Dec 2010 (pp 68-71) http://gjeis.academician.co.in/ ; www.ejournal.co.in/gjeis

[17] Narendra Kumar Tyagi, "Nullifying the Impacts of Security Threats on e-Business using Cryptography with e-BSP" (Track 2: Web Technologies, Computer Networks & Information Security) National conference INDIACOM-2011 at Bharati Vidyapeeth Institute of Computer Applications and Management, Paschim vihar, New Delhi , 10-11th March 2011.